***Транспозиционный шифр***

***Транспозиционный шифр*** – это криптографический алгоритм, в котором порядок алфавитов в открытом тексте перестраивается для формирования зашифрованного текста. В этот процесс фактические алфавиты простого текста не включаются.

Простым примером шифра транспонирования является столбчатый шифр транспонирования, где каждый символ в простом тексте написан горизонтально с заданной шириной алфавита. Шифр написан вертикально, что создает совершенно другой текст шифра.

Рассмотрим простой текст hello world, и давайте применим технику простого столбчатого преобразования, как показано ниже:



Символы простого текста располагаются горизонтально, а зашифрованный текст создается в вертикальном формате: holewdlo lr. Теперь получатель должен использовать ту же таблицу, чтобы расшифровать зашифрованный текст в обычный текст.

Например, слово из трех букв можно переставить только в 6 (= 3!) Различных позициях. Таким образом, «col» можно преобразовать только в «col», «clo», «ocl», «olc», «lco» или «loc». По мере увеличения количества букв количество аранжировок быстро увеличивается, и становится все труднее найти исходный текст без знания перестановки и без каких-либо знаний о открытом тексте. Таким образом, для цифры путем транспонирования, в которой используются блоки по 20 символов, их 20! возможностей, или 2,432,902,008 176,640,000 комбинаций.